DEPARTMENT OF THE NAVY

DIRECTOR NAVAL RESERVE INFORMATION SYSTEMS OFFICE

4400 DAUPHINE STREET
NEW ORLEANS, LOUISIANA 70146-5401

NAVRESINFOSYSOFFINST 5239.1
Code N54

27 JAN 1998

NAVRESINFOSYSOFF INSTRUCTION 5239.1

Subj: INFORMATION SYSTEMS SECURITY GUIDELINES

Ref: (a) SECNAVINST 5239.3
(b) OPNAVINST 5239.1A
(c) NAVSO P-5239-01
(d) COMNAVRESFOR 5239.1A
(e) NAVSO P-5239-04
(f) NAVSO P-5239-07
(g) NAVSO P-5239-08
(h) CNO Message 2120012 Jul 95
(i) DOD 5500.7-R
(j) SECDEF Washington DC 2819282 Jul 97
(k) NAVSO P-5239-29
(l) ASD (C31) Memo of 16 Jan 97
(m) CNO Washington DC 1117542 Oct 95
(n) Advisory 97–10 DOD Site Licensed Anti-Virus Tools
(o) NAVSO P-5239-19
(p) Naval Reserve Logistic Support Handbook P4000.1
(q) SECNAVINST 5211.5D
(r) Public Law 100-235, Computer Security Act of 1987

Encl: (1) Incident Report Sample
(2) Warning Banner

1. Introduction. The Department of the Navy (DON) Information Systems Security (INFOSEC) Program is assigned to comply with, Department of Defense (DOD), and DON INFOSEC policies per references (a) through (c). The Naval Reserve Information System Office (NAVRESINFOSYSOFF) INFOSEC Program is driven by a need to reduce the risk to system resources by identifying their vulnerabilities to specific threats and applying security measures to prevent or reduce the impact on system assets from threat occurrences. NAVRESINFOSYSOFF's INFOSEC Program is directed to ensure that information is protected from unauthorized disclosure, denial of service, destruction, and modification.

2. Scope. The information contained in this document applies to all NAVRESINFOSYSOFF Local Area Network (LAN) and Information Systems (ISs) users including all military, civilian and contractor personnel. This instruction is to define the laws,

rules, significant directives, policies and practices that will govern NAVRESINFOSYSOFF's INFOSEC Program and will set guidance for NAVRESINFOSYSOFF's authorized users. For the purpose of this document, IS resources will include all computer systems, microcomputers, notebooks, laptops etc., and any workstations under NAVRESINFOSYSOFF cognizance.

3. Background. Chartered by the Commander, Naval Reserve Force (COMNAVRESFOR), NAVRESINFOSYSOFF is an Echelon III command responsible for the development, acquisition, implementation, maintenance, and operation of ISs. The Director of NAVRESINFOSYSOFF is dual-hatted as the COMNAVRESFOR Flag Special Assistant for ISs serving as principal advisor and directs all matters related to the development, acquisition, implementation, and operation of Naval Reserve, DOD and Navy ISs.

4. Discussion. Policies are the primary building blocks for all INFOSEC efforts. In order to be successful, a set of policies must be implemented which establishes both direction and management support. The number one key to INFOSEC success is the involvement and support at all levels of management.

4.1. The Designated Approving Authority (DAA) decides if an IS, network or computer resource may operate per references (a) through (c). Permission to operate is granted when the DAA determines that an IS operates at an acceptable level of risk.

a. The Director of NAVRESINFOSYSOFF is the DAA who is responsible for ensuring compliance with the DON INFOSEC Program.

4.2. NAVRESINFOSYSOFF's Information System Security Managers (ISSMs) and the INFOSEC security staff consisting of Information System Security Officers (ISSOs) and the Network Security Officer (NSO) have been identified per references (d) through (g). The INFOSEC staff is further identified below:

a. NAVRESINFOSYSOFF ISSMs functions as the activity's focal point and principal advisor for INFOSEC matters on behalf of the DAA. The ISSMs report to the DAA and implement the overall INFOSEC program as approved by the DAA.

b. The ISSOs acts on behalf of the ISSMs to ensure compliance with the INFOSEC procedures within their area of responsibility at their operation sites or facilities.

c. The NSO acts on behalf of the ISSMs to implement the network security policy of the activity across all data networks and the activity under the NSO's authority.

5. Internet Policy. The current explosive growth of the Internet and the "Information Superhighway" creates a rapidly-changing situation where boundaries between appropriate and inappropriate uses can be blurred. Some institutions have lost stature due to widely-circulated reports of clearly inappropriate activities being conducted on their computer systems and/or repeated break–ins resulting in compromise of their information resources. This situation requires that NAVRESINFOSYSOFF establish clear and explicit policy on appropriate and acceptable uses of its ISs per references (h) through (j).

a. In consideration of its primary mission, NAVRESINFOSYSOFF authorizes use of its IS resources for all purposes reasonably related to accomplishing its mission; intellectual inquiry intended to expand knowledge of current technology and keep abreast of technological innovations which may be of use to current or future customers; to communicate electronically with customers, support contractors, vendors and other agencies with whom the command has an association, so long as that communication is for official purposes. NAVRESINFOSYSOFF staff and contractors are encouraged to make maximum utilization of these resources to increase their professional knowledge, skills, and ability to contribute to mission accomplishment and identifying and implementing cost–effective and/or more efficient ways of performing assigned tasks.

b. NAVRESINFOSYSOFF restricts those uses of its IS resources that are clearly inappropriate in a taxpayer–supported agency, or which are inconsistent with the professional standards expected of its staff and contractors. In any instance involving a question as to whether a specific action or conduct is or was appropriate, the primary consideration should be whether such action or conduct would be consistent with that expected of professional military members and public servants, who realize that their actions reflect not only on themselves, but on NAVRESINFOSYSOFF, the Navy, and DOD as well.

c. Use of command IS resources and network connections constitutes express consent by the user to monitoring, recording, auditing for the purposes of ensuring the systems and networks are functioning properly, protecting against unauthorized access or use, ensuring the confidentiality and integrity of data and information resident on the systems and" networks, and ensuring that any software used complies with copyright agreements per references k and l. Users have no expectation of privacy when using command IS resources or public switched network (i.e. Internet, FTS–2000, etc.).

5.1. Specific Restrictions and Limitations.

a. There are certain activities not in keeping with the NAVRESINFOSYSOFF mission or its status as a Navy activity that they are expressly prohibited on all NAVRESINFOSYSOFF systems or those systems owned by customers or contractors that are operated on behalf of NAVRESINFOSYSOFF. These are:

(1) Illegal, fraudulent, or malicious activities, partisan political activity, political or religious lobbying, activities on behalf of organizations having no affiliation with NAVRESINFOSYSOFF. Action which intentionally cause damage to equipment or introduction of viruses are included in this category.

(2) Activities for the purposes of personal or commercial financial gain not in support of NAVRESINFOSYSOFF or its mission. This includes chain letters, solicitation of business or services, sales of personal property, resumes and other forms of employment applications, etc. not in support of NAVRESINFOSYSOFF or its mission.

(3) Storing, processing, or displaying offensive, disrespectful or obscene material, such as pornography and other sexually explicit material, “hate literature”, etc.

(4) Storing or processing classified information on any system not explicitly approved for classified processing.

(5) Annoying or harassing another individual, i.e. by sending uninvited e-mail of a personal nature or by using lewd or offensive language.

(6) Using another individual’s account or identity without their explicit permission, i.e. by foreging e-mail, logging onto a system/network using their identification and password, cracking other users’ passwords, etc.

(7) Viewing, damaging, or deleting other users’ files or communications without appropriate authorization or permission.

(8) Attempting to circumvent or defeat security or auditing systems, without prior authorization from the command ISSMs and other than as part of legitimate system test or

security search. This includes removing or tampering with virus checking capabilities as configured by Network Administrators, ISSMs, ISSOs and NSO without prior approval or acceptance.

(9) Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's license agreement (i.e. activities that are commonly called "piracy").

(10) Installing legal copies of software expressly prohibited by the Director or by other competent higher authority, without prior permission. Any software purchased by an employee must comply with the software license and registration agreement and be documented with the Command Software Manager. This applies to public domain, customer-owned, personally-owned, government-owned, and shareware software. The Director's approval is assumed on all software procured by the command regardless of the funding source.

(11) Electronically transmitting classified or sensitive information to unauthorized recipients.

(12) NAVRESINFOSYSOFF networks shall not be used to transmit any communication where the meaning of the message, or its transmission or distribution, would violate any policy, applicable law or regulation that would likely be highly offensive to the recipient or recipients thereof.

b. There are certain other activities which are not absolutely prohibited, but are almost always inappropriate. Individuals engaging in such conduct may reasonably expect to be asked to justify their activities, and if reasonable justification does not exist, may find their judgement and/or professional standards seriously questioned. Examples of such generally inappropriate activities are:

(1) Use of NAVRESINFOSYSOFF systems that, in the judgment of the responsible system administrator, seriously interfere with other legitimate uses or users. Examples may include "hogging" systems or actions which cause excessive network slowdowns, excessive large file transfers, excessive personal e-mail, exessive storage of large (i.e. multi-media) non-mission related files, etc.

(2) Storing files or material which could reasonably be used for illegal or fraudulent purposes.

c. Users who participate from NAVRESINFOSYSOFF systems in news groups, bulletin boards, discussion lists, etc. should generally limit such participation to forums related to their own professional expertise or assigned projects and should ensure their contributions are restrained, professional, objective and clearly identified as personal opinions, not official NAVRESINFOSYSOFF, DON, or DOD policies.

5.2. Firewall. Per reference (h) all Navy ISs with servers (including web servers) which are connected to unclassified publicly accessible computer networks such as the Internet, will employ appropriate security safeguards (such as a firewall) as necessary to ensure the integrity, authenticity, privacy and availability of a command's IS and its data. A firewall that is properly installed, configured, and maintained can be expected to perform reliably in accordance with the policies, rules, access lists and authorization criteria that have been established and set up for its effective operation.

5.3. WebPage Access. WebPages provide the public with user-friendly graphics-based multi-media access to information on the Internet, and is the most popular means for accessing, storing and linking Internet-based information in practically any format. Information placed on any NAVRESINFOSYSOFF WebPage shall be unclassified, and have a clearly defined purpose related to the mission of the organization per reference (j) and should strive to be accurate and as current as possible.

6. E-Mail Policy. Electronic Mail provides an effective way to pass and chronicle inter- and intra-organizational communications. This policy clearly describes NAVRESINFOSYSOFF command guidelines regarding access to and the disclosure of messages sent or received by employees while using the command's E-mail system per references (h) through (i). All NAVRESINFOSYSOFF's personnel shall not use an E-Mail account assigned to another individual to either send or receive messages (except as authorized by the account owner or by authorized higher authority). The intent of this policy is to reinforce the notion that each user should have their own E-mail account, and that users should not share these accounts per references (h) through (i).

a. Management's Right to Access Information. The E-mail system has been installed by NAVRESINFOSYSOFF to facilitate command communications. Although each' employee has an individual password to access this system, the contents of any E-mail is accessible at all times by NAVRESINFOSYSOFF for any official command purpose. The command does reserve the right to inspect, copy, store, and disclose the contents of E-mail messages at **any** time. However, it will do so only when it believes it is appropriate to prevent or correct improper use, satisfy a legal obligation, or ensure proper operation of the E–Mail facilities per references (h) and (i).

(1) The E-mail system may be subject to periodic unannounced inspections, and should be treated like other shared filing systems. All system passwords and encryption keys must be available to command management. Installation of encryption programs or encrypted files will not be used without first providing such appropriate keys to the ISSMS. Copies of all keys will be kept under restricted access and be utilized for emergency or legitimate purposes at the direction of the Department Director or by competent higher authority. All E-Mail messages are command records, contents properly obtained for legitimate business purposes may be disclosed within the command without your permission. Therefore, you should not assume that messages are private. Back-up copies of E-mail are regularly completed, maintained and referenced for official and legal reasons.

(2) When necessary for the maintenance of a system or network, system administrators may restrict availability of shared resources. It may also be necessary to access a user's files to resolve or follow-up on reported problems.

b. Personal Use of E-mail. Some reasonable personal use IS may be authorized. Examples of authorized personal use include reasonable communications by civilian, military and contract personnel while traveling on U.S. Government business to notify family members of official transportation or schedule changes. They also include personal communications from the employee's workplace that are reasonably made while at work, such as checking in with spouse or minor children, scheduling doctor, auto, or home repair appointments, brief Internet searches, etc.

(1) NAVRESINFOSYSOFF provides the E-mail system to assist you in the performance of the command's mission. Incidental and occasional personal use of E–mail may be permitted, but these uses shall not interfere with the mission of the command and will be treated the same as other messages: NAVRESINFOSYSOFF reserves the right to access and disclose as necessary all messages sent over its E–mail system, without regard to content. Since personal messages can be accessed by NAVRESINFOSYSOFF management without prior notice, you should not use E-mail to transmit any messages you would not want read by a third party. For example, you should not use the command E-mail system for personal or medical information about yourself or others likely to embarrass

the sender, or cause undue emotional duress of others. In any event, you shall not use these systems for such purposes of soliciting for commercial ventures, religious, political or personal causes or external organizations or other similar, non-job-related solicitations. Misuse of any NAVRESINFOSYSOFF system may subject you to disciplinary action.

(2) Any user of the E-mail system whose actions involving E–mail that violate this policy, or any other related command policy or regulation, may be subject to limitations or elimination of E-mail privileges as well as other disciplinary actions.

c. Forbidden Content of E–mail Communications. You may not use NAVRESINFOSYSOFF ISs in any manner that may be reasonably seen as insulting, disruptive, offensive by other persons, harmful to morale or in any way detrimental to good order and discipline. Examples of forbidden transmissions include sexually–explicit messages, photographs, cartoons, or jokes, ethnic or racial slurs, or any other message that can be construed to be harassment or ridicules others based on their sex, race, sexual orientation, age, national origin, or religious or political beliefs. In addition, the following specific actions and use of E-mail are improper, and violations may result in disciplinary action:

(1) Concealment or misrepresentation of names or affiliations in E–mail messages.

(2) Alteration of source or destination address of E-mail.

(3) Use of E-mail facilities for commercial or private business purposes, or “underground” organizations.

(4) Use of E-mail which unreasonably interferes with or threatens other individuals.

(5) Use of E-mail that degrades or demeans other individuals.

(6) Transmission of fraudulent, harassing or obscene messages and/or materials. These messages are not to be sent, printed, requested or stored.

(7) Any use congesting the E-mail system that would deprive others of resources is prohibited.

(8) Chain letters and other forms of unapproved mass mailings.

(9) Storing or processing classified information on systems not explicitly approved for classified processing. Classified data is not permitted on the NAVRESINFOSYSOFF E-mail system.

7. Virus Scanning Policy. This policy describes NAVRESINFOSYSOFF command guidelines regarding anti-virus and virus eradication efforts: to reduce the risk of introducing malicious code into command owned/operated ISs; to reduce any resultant damage and contain the spread of such software per references (m) thru (o). A computer virus is a malicious software which can hide itself in other executable software (including macros) and then cause that software to make copies of the virus.

7.1. To protect our IS assets against virus infection, we will use the three step approach:

a. Prevention - those steps necessary to limit or prevent exposure to viruses.

b. Detection – those steps necessary to detect infections in order to limit the spread and impact.

c. Response/recovery - those steps necessary to remove the virus and restore the ISs and files to normal operation.

7.2. Methods of Transmission. The most common method of spreading a virus from one computer to another is through the exchange of infected floppy diskettes. A virus can also be transferred by direct access to another computer (through a network or modem). The following are common sources of viruses:

a. Files downloaded from Bulletin Board Systems (BBSS), online services, and Internet sites.

b. Preloaded software shipped on a new computer.

c. Demonstration/evaluation software received from vendors.

d. Diskettes used by service or support technicians.

e. Pirated (i.e. illegal) software acquired from friends or co–workers.

f. Shareware diskettes received from mail order catalog companies.

g. Computer stores selling returned software as new.

h. Diskettes used in friends or co–workers computers.

i. Exchange of infected files on a network.

j. Specific acts of sabotage by disgruntled employees.

k. College campus computer laboratories.

l. Using infected backups.

m. Remote access to infected computers.

n. Government-owned and distributed software.

7.3. The use of command anti-virus software is mandatory for any microcomputer used within the scope of this policy. This includes all IS resources accessing from remote sites. Reference (n) identifies the current DOD site licensed approved anti-virus software for use on NAVRESINFOSYSOFF microcomputers and may also be used by all DOD personnel on their home personal computers. The anti-virus software shall be configured to scan the hard–drive(s) on first boot each day the system is turned on and remain memory Terminate-and–Stay–Resident (TSR) while the computer is in operation. Waivers for this requirement must be approved in writing by the ISSMs based on demonstrated and valid reason (insufficient memory, memory conflicts or other conflicts with application software used on the system, etc.). System response time is not a valid justification for removing anti-virus scanning capabilities.

7.4. Files downloaded from remote sources (BBS, networks, online service, etc.), or received on diskettes from sources outside this command shall be scanned for viruses upon receipt/download before being executed on any computer. Diskettes brought from users' home computers are included in this category.

7.5. Any server that is connected to NAVRESINFOSYSOFF LAN must be protected by command standard anti-virus software.

8. Diskette Label (External Labeling). Implementation requirements for the INFOSEC Program centers around the classes of data processed at NAVRESINFOSYSOFF and the requirements governing its protection. Central Processing Units (CPUs) will

accurately reflect (label) the highest level of information stored and/or processed as stated in this policy. NAVRESINFOSYSOFF personnel will label all diskettes with user name, extension and department code.

9. Desktop Policy. To provide NAVRESINFOSYSOFF with the information necessary to operate and use their ISs securely per reference (a), all NAVRESINFOSYSOFF personnel shall comply with and ensure ISs within their area of responsibility are covered by these procedures.

9.1 Information Systems Custodian.

a. To comply with references (a) and (p), NAVRESINFOSYSOFF utilizes the Control Equipage Inventory System (CEIS) to ensure proper accountability of controlled minor property (including hardware and software control, physical inventory distribution and usage controls) . Changes in the status of any NAVRESINFOSYSOFF property shall be completed per applicable laws and regulations, NAVRESINFOSYSOFF resource management policy and documented by individual internal transfer worksheet or other appropriate, authorized transfer documentation.

b. NAVRESINFOSYSOFF ISs are authorized to process Official Use Only, Unclassified and Sensitive Unclassified data. This security desktop procedure represents the minimum requirements for ISs that process exclusively unclassified and sensitive unclassified data. Any changes in the level of data processed utilizing NAVRESINFOSYSOFF equipment are not authorized without prior specific written approval from NAVRESINFOSYSOFF N00 and ISSMs.

9.2. Physical Security/Access Control. Most NAVRESINFOSYSOFF ISs are located in government secured workspaces. All personnel are required to carry government issued coded identification badges. Each office door is equipped with a cipher lock, combination cipher lock, door key, or card access system. Personnel are responsible to ensure reasonable actions are taken to provide for physical security and access controls for all ISs under their area of responsibility.

9.3. Good Security Practices.

a. Passwords recommendations:

(1) Change passwords frequently. The longer you use the same passwords, the higher the risk of compromise. Password changes of every (90) days is a good rule of thumb.

(2) Use a combination of numbers and letters (Caps and lower case too, if permitted). Do not use common words (i.e. password), persons (i.e. your name), places (i.e. NAVRESINFOSYSOFF), dates, numbers, or other words that can be closely identified with you.

(3) At a minimum, use six to eight characters in length for passwords.

(4) Safeguard and do not share passwords.

b. Inspect your data and equipment. If you have reason to suspect someone may have tampered with your equipment, files or data, report it immediately to your departmental ISSO or ISSM.

c. Do not leave sensitive data in a IS or place on diskettes that does not afford adequate access controls or proper security.

d. Ensure all ISs have adequate security measures, especially in unoccupied spaces.

e. Avoid keeping magnets, liquids and food in the immediate vicinity of the ISs. Foods and liquids dropped on or into ISs (including keyboards) can cause malfunctions and destruction of property and files. Magnets are also capable of causing malfunctions and destruction of electronic files.

f. Report any suspected IS misuse or abuse to your departmental ISSO or ISSM. Whether directed against you or not, abuse or misuse of command IS resources hinders the timely completion of your task.

9.4. Standard Operating Procedures.

a. All authorized individuals utilizing IS equipment must be made aware of security procedures prior to operating any NAVRESINFOSYSOFF resource. The following procedures are applicable to all authorized users:

(1) All diskettes, compact disks (CD), and software are to be secured during non-working hours and when not in use.

(2) A warning label indicating the highest level of information processed in each IS will be affixed to the CPU.

(3) Backup of all important data should be performed on a weekly basis or more often if appropriate.

(4) Ensure that each microcomputer is equipped with a surge protector.

9.5. Media Protection.

a. Media (5 1/4" floppy diskettes, 3 1/2" diskettes, CD's and cartridge tapes will be handled with care and stored in their protective jacket (if appropriate) at all times when not in use.

b. Protect from bending or similar handling. Do not use magnets, rubber bands or paper clips which may cause damage.

c. Avoid contact with objects which have magnetic fields (i.e., etc. telephone instruments).

d. Avoid writing with ball-point pens, pencils or similar instruments either directly or through the protective jacket.

e. Label appropriately.

f. Do not force or bend media when inserting into a drive.

9.6. Media Input/Output and Declassification or Destruction.

a. All personnel are to ensure that hard copies of all Privacy Act data are properly stored and disposed of. Per reference (q), all users are to be aware of releasable information for NAVRESINFOSYSOFF personnel.

b. All diskettes that contain sensitive unclassified or privacy act information are to be adequately protected and should only be discarded in regular waste containers after ensuring the media and data has been adequately cleared or rendered useless.

9.7. Virus Protection. The following instructions apply:

a. All ISs (i.e. workstations, stand-alone, etc.) will have loaded and utilize the latest version of virus scanning software authorized as provided by NAVRESINFOSYSOFF INFOSEC office.

b. All new incoming computers will be scanned and have installed the current authorized version of virus scanning software as part of their initial setup.

c. Users will acquaint themselves with the proper use of the virus scanning software to prevent the spread of computer viruses.

d. All systems should be scanned daily (recommend at initial logon).

e. All diskettes should be scanned prior to other access.

f. Departmental ISSOs shall:

1. Identify all microcomputers within their department and ensure the current approved anti-virus software is installed and operating.

2. Compile all information needed to supply the Fleet Information Warfare Center's, Naval Computer Incident Response Team (NAVCIRT) with an Incident Report, per enclosure (1).

g. ISSMs shall:

1. Ensure applicable information is provided to NAVCIRT in a timely, accurate manner.

2. Conduct random software license, virus and system audits.

3. ISSMs will provide the departmental ISSOs with updated versions of authorized virus scanning software.

4. Ensure command INFOSEC training is provided.

9.8. Individual IS Contingency Planning (CP). Contingency planning is an integral phase of an activity's INFOSEC Program. CP is required for all ISs, networks or other computer resources that are essential to the performance of an activity's mission. The following elements will assist all NAVRESINFOSYSOFF personnel tasked with providing information systems services during times of disruption of normal IS operations.

a. In the event your IS becomes inoperative:

1. Call the Customer Support Center (CSC) at 678-7070 or 1-800-537-4617.

2. Provide your name, building/room number, and extension.

3. Give a brief description of the problem.

4. Obtain the name of the CSC representative assisting you.

5. The CSC representative will provide you with a trouble ticket number; refer to this number when any future inquiries are placed.

b. Any significant changes in hardware/software configuration, classification level of processed data, operating mode/posture, etc. requires a re–evaluation of the IS, and should be promptly reported to your departmental ISSO or command ISSMs.

10. Warning Banner. DOD mandates the use of a warning banner on all ISs as stated in reference (1). The warning banner is intended to confirm to the user that all data contained on DOD systems are subject to review by DOD security and/or system administrator personnel and ensure that computer users are aware of system monitoring. The lack of proper warning banners may result in the violation of federal wiretap and privacy statutes. This applies to all networked and stand-alone DOD systems, both government and contractor owned, that access government data files. The file and any updates are available from your departmental ISSo or ISSM. The banner should be displayed at system initialization. All personnel shall ensure that the banner is displayed on all systems (workstations, servers, stand-alone, etc.). Enclosure (2) is provided for your information.

11. INFOSEC Training and Awareness. Reference (r) mandates training for all personnel responsible for the input and use of government resources. There shall be in place, a security training and awareness program for the security requirements for all persons accessing ISs per references (a) and (b). The INFOSEC staff will develop and maintain the NAVRESINFOSYSOFF INFOSEC program. The security training program will include a mixture of security videos, oral classroom presentations, annual awareness training (briefs), E-mail security messages, plan of the week (POW) notes, and security posters.

12. Responsibilities. All NAVRESINFOSYSOFF system users are responsible for adhering to this policy. Individual users who violate this policy may be subject to various penalties, ranging from informal counseling, to revocation of NAVRESINFOSYSOFF IS user privileges and resources, to formal disciplinary action,

including reprimands, fines, non-judicial punishment court-martial of military personnel, or removal for cause of civilian/ contractor personnel. In all cases, users are accountable for their actions.

a. Supervisors will apprise their employees of this policy and ensure that the controlled use of IS assets is under their respective jurisdiction.

b. The ISSMs will include training on this policy during indoctrination orientation and ensure refresher training during annual INFOSEC security training.

c. Contracting Officer's Representatives will apprise their contractors of this policy and their responsibilities.

d. The LAN Administrator and NSO will monitor user's files and e-mail in cases where network/data security are in question and assist ISSMs with investigations as necessary.

e. The Software and Resource Manager will ensure that all software is accounted for, properly licensed and any unauthorized software is promptly removed or legally licensed on all command ISs.

f. Privileged users are those having "super-user", "root", or equivalent access to a system which give them complete or near–complete control of the operating system. To ensure the security and integrity of data, administraors have greater responsibilities to monitor, avoid and prevent improper access to, and misuse of computational resources under their control.

12.1. Action. Supervisors will give this policy widest dissemination and ensure that their employees comply with its provisions.

a. Actual or alleged violations of, or questions regarding the applicability of this policy will be addressed through normal command channels. The ISSMs will investigate any incidents that are security related. The Software Manager, with advice from the ISSMs, will make determinations concerning legal software usage issues. The DAA will make the final determination in all instances that cannot be adequately resolved at lower levels.

13.0. Summary/Conclusion. The intention of this policy is to clearly communicate to all NAVRESINFOSYSOFF personnel that

INFOSEC is multi-departmental, multi-disciplinary, and multi-organizational. Therefore, all NAVRESINFOSYSOFF's personnel should be specifically charged with the responsibility of INFOSEC in order to achieve appropriate levels of security.

D. A. WIKENHEISER

Distribution: (NAVRESINFOSYSOFFINST 5216.1)
List A
List B
List C

SAMPLE

COMPUTER INCIDENT REPORT

1. The following information is provided on the IS viruses.

(a) Name of infecting virus: Form

(b) Source of the virus, date detected: The Form virus was detected on one 3.5” diskette in the F. C. Management Department on 2 Jun 97. In an attempt to read a file, a diskette provided by N55, the IBM Anti-Virus (IBMAV) software detected the Form virus. When the user received the message “Infected boot records were found”, employee immediately notified the Information System Security Officer (ISSO) who assisted in the documentation and virus removal.

(c) Other locations, within or outside of the command, was possibly infected as a result of this virus:

(1) The originator of the diskette was notified and the IBMAV software was installed on his IS.

(d) Number and types of systems infected: (1) 3.5” diskette

(e) Method of clean-up: IBMAV Clean

(f) Number of man-hours required in effort: 5 minutes

(g) Damage or observations resulting from the virus triggering: None

(h) Command name and location:

Director, Naval Reserve Information System Office
4400 Dauphine St.
New Orleans, LA 70146-5401

(i) Point of contact: (Reporting ISSM’s Name)
DSN: 678-4444 Comm: (504)678-4444
Information System Security Manager (ISSM)

SAMPLE

NOTICE AND CONSENT LOG-ON BANNER

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTERS SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THEIR SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED.

USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THE SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAYBE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20350-1000

SECNAVINST 5239.3
NISMC
14 JULY 1995

SECNAV INSTRUCTION 5239.3

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM

Ref: (a) DODD TS3600.1 of 21 Dec 92, Information Warfare (NOTAL)
(b) P.L. 100-235 of 8 Jan 88, Computer Security Act of 1987
(c) OMB Circular A-130 of 15 Jul 94, Management of Federal Information Resources (NOTAL)
(d) NSTISSID No. 500 of 25 Feb 93, Telecommunications and Automated Systems Security Education, Training and Awareness
(e) NSTISSD No. 501 of 16 Nov 92, National Training Program for Information System Security (INFOSEC) Professionals
(f) NSTISSD No. 502 of 5 Feb 93, National Security Telecommunications and Automated Information Security
(g) NSTISSP No. 6 of 8 Apr 94, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems, (NOTAL)
(h) DODD 5200.28 of 21 Mar 88, Security Requirements for Automated Information Systems (AISs) (NOTAL)
(i) DODD C-5200.5 of 21 Apr 90, Communication Security (COMSEC) (NOTAL)
(j) DODD C-5200.19 of 23 Feb 90, Control of Compromising Emanations (NOTAL)
(k) DODD 5000.2 of 23 Feb 91, Defense Acquisition Policies and Procedure (NOTAL)
(l) CJCSI 6510.01 of 1 Sep 93, Chairman of the Joint Chiefs of Staff Instruction, Joint and Combined Communications Security (NOTAL)
(m) NSTISSI 4009 of 5 Jun 92, National Information Systems Security (INFOSEC) Glossary (NOTAL)
(n) SECNAVINST 5000.2A of 9 Dec 92, Implementation of Defense Acquisition Management Policies, Procedures, Documentation, and Reports (NOTAL)
(o) SECNAVINST 5231.1C of 10 Jul 93, Life Cycle Management Policy and Approval Requirements for Information System Projects
(p) SECNAVINST 5200.32A of 3 May 93, Acquisition Management Policies and Procedures for Computer Resources

Encl: (1) List of Acronyms
(2) Glossary of Terms

DEPARTMENT OF THE NAVY
AUTOMATIC DATA PROCESSING SECURITY PROGRAM

UNITED STATES NAVY
CHIEF OF NAVAL OPERATIONS

OPNAVINST 5239.1A

AUG 3 1982

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS

Department of the Navy
Naval Information Systems
Management Center

NAVSO P-5239-01
May 1995

INTRODUCTION TO

INFORMATION SYSTEMS SECURITY

(INFOSEC)

GUIDEBOOK

MODULE 01

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

0515-LP-208-8200

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer
Naval Command, Control and Ocean Surveillance Center

DEPARTMENT OF THE NAVY
COMMANDER NAVAL RESERVE FORCE
NEW ORLEANS. LOUISIANA 70146-5000

COMNAVRESFOR INSTRUCTION 5239.1A

Subj: NAVAL RESERVE FORCE AUTOMATED INFORMATION SYSTEMS SECURITY PROGRAM

Ref: (a) DODDIR 520.28,Security Requirements for Automated Information Systems (NOTAL)
(b) OPNAVINST 5510.1H, DON Information and Personnel Security Program
(c) OMB Circular A-130 Management of Federal Information Resources (NOTAL)
(d) DODINST 5215.2, Computer Security Technical Vulnerability Reporting Program (CSTVRP) (NOTAL)
(e) P.L. 100-235, Computer Security Act of 1987
(f) SECNAVINST 5239.~~2~~3 DON Automated Information Systems (AIS) Security Program
(g) OPNAVINST 5239.1A, DON Automatic Data Processing (ADP) Security Program
(h) DOD 5200.28-STD, Trusted Computer System Evaluation Criteria (NOTAL)
(i) OPNAVINST C5510.93E, Navy Implementation of National Policy on Control of Compromising Emanations
(j) COMNAVRESFORINST 5500.3, Naval Reserve Force Security Manual
(k) CNO Washington 241959Z Jan 86 (NAVOP 006/86) (canceled 24 Apr 86)
(l) CSP–1, Communications Security Policy Manual
(m) OPNAVINST 5530.14B, DON Physical Security and Loss Prevention

Encl: (1) Definition of Terms
(2) Minimum Program Requirements
(3) Related Documents
(4) Incident and Vulnerability Report Format (A

1. Purpose

a. To establish the Naval Reserve Force Automated Information Systems (AIS) Security Program.

b. To define the organizational structure to execute the Naval Reserve Force AIS Security Program.

c. To issue policies and guidelines necessary for consistent and effective implementation throughout the Naval Reserve.

d. To apply basic policy and principles of security as they relate to computer-based systems which handle classified, sensitive unclassified, and unclassified information.

Department of the Navy
Naval Information Systems
Management Center

NAVSO P-5239-04
September 1995

INFORMATION SYSTEMS SECURITY

MANAGER (ISSM)

GUIDEBOOK

MODULE 04

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

DEPARTMENT OF THE NAVY

NAVSO P-5239-07

FEBRUARY 1996

INFORMATION SYSTEMS SECURITY

OFFICER (ISSO)

GUIDEBOOK

MODULE 07

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

DEPARTMENT OF THE NAVY

NAVSO P-5239-08
MARCH 1996

NETWORK SECURITY OFFICER (NSO)

GUIDEBOOK

MODULE 08

INFORMATION SYSTEMS SECURITY (INFOSEC)
PROGRAM GUIDELINES

ADMINISTRATIVE MESSAGE

ROUTINE

R 212001Z JUL 95 ZYB MIN

FM CNO WASHINGTON DC//N6//

TO ALCOM

THIS IS A 2 PART MSG COLLATED BY MDS
UNCLAS //N02250//
ALCOM 035/95

MSGID/GENADMIN/CNO WASH DC N643//

SUBJ/GUIDELINES FOR NAVAL USE OF THE INTERNET//

REF/A/DOC/SECNAV/870603//

REF/B/DOC/SECNAV/920617//

REF/C/DOC/CNO/880429//

REF/D/DOC/CNO/930430//

REF/E/DOC/CNO/850401//

NARR/REF A IS SECNAVINST 5720.44A U.S. NAVY PUBLIC AFFAIRS REGULATIONS. REF B IS SECNAVINST 5211.5D DEPARTMENT OF THE NAVY PRIVACY ACT PROGRAM. REF C IS OPNAVINST 5510.1H DEPARTMENT OF NAVY INFORMATION AND PERSONNEL SECURITY PROGRAM REGULATION. REF D IS OPNAVINST 2710 NAVY LOCAL AREA NETWORKS POLICIES. REF E IS OPNAVINST 5239.1A ADP SECURITY POLICY.//

RMKS/1. THE DOD AND DON ARE CURRENTLY IN THE MIDST OF WHAT IS COMMONLY CALLED THE INFORMATION EXPLOSION. THE EXPONENTIAL GROWTH OF THE INTERNET AND THE WORLD WIDE WEB (WWW OR WEB) IS IN PART DUE TO THE EASE OF THE USE AND POPULARITY OF HYPERTEXT BROWSING APPLICATIONS. HYPERTEXT INTERNET APPLICATIONS MAY IMPROVE MANY FACETS OF OUR OPERATIONS, AND PROVIDE AN EFFICIENT AND EFFECTIVE MEANS OF COMMUNICATION AND INFORMATION DISTRIBUTION. THE NATIONAL INFORMATION INFRASTRUCTURE (NII) AND THE DEFENSE Information INFRASTRUCTURE (DII) HAVE AS A GOAL TO INCREASE THE EASE AND AVAILABILITY OF INFORMATION, BOTH WITHIN THE GOVERNMENT AND TO INFORMATION APPROVED FOR PUBLIC RELEASE AND ACCESSIBILITY BY THE PUBLIC.

2. EASY TO USE WEB BROWSERS AND SOFTWARE TOOLS TO EASE THE DEVELOPMENT OF DOCUMENTS WRITTEN IN HYPERTEXT MARKUP LANGUAGE (HTML) HAVE GIVEN RISE TO A PROLIFERATION OF WWW HOME PAGES ON THE INTERNET, INCLUDING MANY BY NUMEROUS NAVY COMMANDS OPERATING IN THE DOMAIN NAME NAVY.MIL. COUPLED WITH THEIR PROMISED BENEFITS HOWEVER,

SERVICES SUCH AS WWW, HYPERTEXT TRANSFER PROTOCOL (HTTP), GOPHER, ANONYMOUS FILE TRANSFER PROTOCOL (FTP), AND OTHER OPEN ANONYMOUS INFORMATION SERVERS PRESENT POTENTIAL PROBLEMS:

(A) DEPENDING ON THE SIZE OF THEIR INFORMATION FILES AND THE EXTERNAL DEMAND FOR THESE FILES, SUCH SERVICES CAN CONSUME SIGNIFICANT NETWORK BANDWIDTH, AND SERIOUSLY DEGRADE NETWORK PERFORMANCE FOR OTHER SYSTEMS SHARING THE SAME NETWORK COMPONENTS, AND POTENTIALLY DEGRADE OR DENY ACCESS TO REQUIRED INFORMATION BY INTERNAL USERS.

(B) TO BE USEFUL, SUCH SERVERS MUST ACCEPT OUTSIDE USERS WITHOUT REQUIRING EITHER A LOCAL USER ACCOUNT OR PASSWORD. PROVIDING SUCH SERVICE CLEARLY ENTAILS SECURITY RISKS, RISKS TO WHICH THE DON MUST BE ESPECIALLY SENSITIVE BECAUSE MILITARY COMPUTER SYSTEMS ARE TRADITIONALLY HIGH PROFILE TARGETS. tHE CONNECTION OF NAVAL INFORMATION SYSTEMS AND NETWORKS TO UNCLASSIFIED PUBLICLY ACCESSIBLE COMPUTER NETWORKS AND INFORMATION SYSTEMS POSES A POTENTIAL THREAT TO NAVAL OPERATIONS. WE CANNOT VIEW THESE CONNECTIONS AS RISK-FREE. THE POTENTIAL EXISTS NOT ONLY FOR UNAUTHORIZED PERSONS TO GAIN ACCESS TO NAVAL INFORMATION SYSTEMS, BUT FOR THE INADVERTENT DISCLOSURE OF CLASSIFIED, UNCLASSIFIED BUT SENSITIVE, AND PRIVACY INFORMATION, AND THE COMPROMISE OF NAVAL OPERATIONS AND ACTIVITIES AS WELL. REQUIRING A LOCAL USER ACCOUNT OR PASSWORD PRIOR TO ACCESSING DATA AVAILABLE ON THE INTERNET IS NOT IN ITSELF A SUFFICIENT SAFEGUARD. IT IS IMPERATIVE THAT THE DEPARTMENT OF THE NAVY ENDEAVOR TO EVALUATE THE RISK AND ENSURE THAT DUE CARE IS TAKEN TO MINIMIZE THE CHANCE OF COMPROMISE.

3. IT IS FULLY APPROPRIATE FOR NAVAL COMMANDS TO ESTABLISH AND MAINTAIN INFORMATION SERVERS AND SERVICES ON THE INTERNET, INCLUDING WORLD WIDE WEB HOME PAGES WITH LINKS TO OTHER PAGES, PROVIDED THEY SUPPORT LEGITIMATE, MISSION-RELATED ACTIVITIES OF THE NAVY AND MARINE CORPS, AND ARE CONSISTENT WITH PRUDENT OPERATIONAL AND SECURITY CONSIDERATIONS. ONE TYPE OF LINK THAT MUST BE AVOIDED IS THE LINK TO A SPECIFIC VENDOR WHO IS SELLING SERVICES AND PRODUCTS TO THE GOVERNMENT, AS THAT TYPE OF LINK MAY GIVE THE APPEARANCE THAT THE DON IS ENDORSING THE PRODUCT OR SERVICE, OR SHOWING FAVOR TO A PARTICULAR VENDOR. INFORMATION PLACED ON THE INTERNET, WITHOUT CONTROLS TO ELIMINATE OR PREVENT PUBLIC ACCESS, MUST BE CLEARED IN A MANNER CONSISTENT WITH THE PROCEDURES ALREADY IN PLACE FOR CLEARING "HARD" COPY INFORMATION. (SEE REFS (A), (B), AND (C)). IN MOST CASES, MATERIAL PROPOSED TO BE MADE AVAILABLE ELECTRONCALLY TO THE PUBLICLY ACCESSIBLE INTERNET MUST BE SUBMITTED THROUGH THE SAME PUBLIC AFFAIRS CHANNELS AS "HARD" COPY MATERIAL PROPOSED FOR PUBLICATION,(FOR NATIONAL RELEASE).

(A) COMMANDERS/COMMANDING OFFICERS MUST ENSURE THAT INFORMATION PROVIDED ON ANY OF THEIR INFORMATION SERVERS CONNECTED TO THE INTERNET, DOES NOT CONTAIN CLASSIFIED, UNCLASSIFIED SENSITIVE, OR PRIVACY INFORMATION, OR INFORMATION THAT COULD ENABLE THE RECIPIENT TO INFER CLASSIFIED OR UNCLASSIFIED SENSITIVE INFORMATION, EITHER FROM INDIVIDUAL SEGMENTS OF THE INFORMATION, OR FROM THE AGGREGATE OF ALL THE INFORMATION AVAILABLE.

(B) ANY INFORMATION PROVIDE THROUGH INTERNET SERVICES MUST BE

PROFESSIONALLY PRESENTED, CURRENT, ACCURATE AND FACTUAL, AND RELATED TO THE COMMAND'S MISSION. COMMANDS MAY CHOODE TO PRODUCE PERIODIC WRITTEN GENERAL GUIDELINES AND PARAMETERS FOR THEIR AUTHORIZED USERS OF UNCLASSIFIED PUBLICLY ACCESSIBLE COMPUTER NETWORKS SUCH AS THE INTERNET. THIS GUIDANCE WILL INDICATE THOSE TOPICS (SUCH AS SENSITIVE INFORMATION ASSOCIATED WITH THE COMMAND'S MISSION OR FLEET OPERATIONS, OR OTHER SENSITIVE DON BUSINESS), WHICH MAY BE RESTRICTED OR PROHIBITED FROM BEING DISCUSSED PUBLICLY OVER NETWORKS.

(C) EACH WEB HOME PAGE WILL HAVE A DESIGNATED AUTHOR OR MAINTAINER WHO WILL BE RESPONSIBLE FOR THE CONTENT AND APPEARANCE OF THAT PAGE. THE INDIVIDUAL'S NAME, ORGANIZATIONAL CODE, ORGANIZATIONAL PHONE NUMBER, EMAIL ADDRES, AND DATE OF LAST REVISION WILL BE INCLUDED IN THE SOURCE CODE FOR THAT PAGE. THE ORIGINATORS OF ANY MATERIAL PROPOSED FOR DISTRIBUTION OR POSTING TO A WEB HOME PAGE, ARE RESPONSIBLE FOR OBTAINING APPROVAL RELEASE, PRIOR TO SUBMITTING THE MATERIAL TO THE WEB SERVER ADMINISTRATOR.

(D) PUBLICLY ACCESSIBLE NEWSGROUPS, BULLENTIN BOARDS, AND EMAIL MAILING LISTS THAT ARE OPERATED BY A COMMAND SHOULD ALSO REFLECT A HIGH LEVEL OF PROFESSIONALISM. INDIVIDUAL USERS WHO SUBMIT EMAIL POSTINGS TO THESE NAVY AND MARINE CORPS OPERATED AND MAINTAINED PUBLICLY ACCESSIBLE NEWSGROUPS AND BULLETIN BOARDS, ARE NOT AUTHORIZED TO SUBMIT CLASSIFIED, UNCLASSIFIED SENSITIVE, OR PRIVACY INFORMATION . COMMANDERS/COMMANDING OFFICERS SHOULD ESTABLISH PROCEDURES FOR PERIODIC REVIEW OF THE CONTENT OF POSTINGS THAT HAVE BEEN MADE TO THESE NEWSGROUPS AND BULLETIN BOARDS OPERATED BY THEIR COMMAND TO ENSURE THE POSTINGS DO NOT BRING DISCREDIT TO THE COMMAND AND THE DON. ALL NAVY AND MARINE CORPS EMAIL USERS SHOULD STRIVE TO ENSURE THAT THE CONTENT OF EMAIL MESSAGES REFLECT A HIGH LEVEL OF PROFESSIONALISM AND PERSONAL INTEGRITY.

4. INFORMATION SYSTEMS SECURITY GUIDELINES:

(A) ALL NAVAL INFORMATION SYSTEMS WITH SERVERS (INCLUDING WEB SERVERS) WHICH ARE CONNECTED TO UNCLASSIFIED PUBLICLY ACCESSIBLE COMPUTER NETWORKS SUCH AS THE INTERNET, WILL EMPLOY APPROPRIATE SECURITY SAFEGUARDS (SUCH AS FIREWALLS) AS NECESSARY TO ENSURE THE INTEGRITY, AUTHENTICITY, PRIVACY, AND AVAILABILITY OF A COMMAND'S INFORMATION SYSTEM AND ITS DATA.

(B) ALL INFORMATION SYSTEMS WITH SERVERS CONNECTED TO THE INTERNET MUST HAVE A FORMAL COMMANDER/COMMANDING OFFICER, OR DESIGNATED APPROVING AUTHORITY (DAA) AUTHORIZATION TO OPERATE. IN ACCORDANCE WITH OPNAVINST 5239.1 (REF (E)), ALL SYSTEMS MUST RECEIVE SECURITY ACCREDITATION AND AUTHORIZATION TO OPERATE BY THE DAA PRIOR TO BEING PUT INTO OPERATION. A NETWORK RISK ANALYSIS MUST BE CONDUCTED AS A PART OF THE OVERALL NETWORK SECURITY PLAN TO DETERMINE THE APPROPRIATE LEVEL OF SECURITY. DON WAN/LAN SYSTEMS SECURITY ACCREDITATIONS MUST BE UPDATED TO REFLECT THE ADDITION OF, OR EXISTENCE OF, A WEB SERVER OR OTHER INTERNET INFORMATION SERVER.

5. SINCE THE INTERNET IS OPEN AND LEGALLY ACCESSED BY THE WORLD-WIDE PUBLIC, INFORMATION PRESENTED BY NAVAL COMMANDS IN THEIR HOME PAGES ON THE INTERNET WILL REFLECT ON THE DEPARTMENT OF THE

NAVY'S PROFESSIONAL STANDARDS AND CREDIBILITY. REGARDLES OF HOW OR BY WHOM THESE PAGES ARE ACTUALLY DEVELOPED, THE APPEARANCE OF, AND THE ACCURACY, CURRENCY, AND RELEVANCE OF THIS INFORMATION WILL REFLECT DIRECTLY, OR INDIRECTLY, ON THE DEPARTMENT OF THE NAVY'S IMAGE. INFORMATION RESIDING ON A SERVER WITH A NAVY.MIL DOMAIN OR USMC.MIL DOMAIN, OR ANY OTHER NAVY OR MARINE CORPS OWNED AND OPERATED SERVER, MAY BE INTERPRETED BY THE WORLDWIDE PUBLIC, INCLUDING THE AMERICAN TAXPAYER AND MEDIA, AS REFLECTING OFFICIAL DEPARTMENT OF THE NAVY, OR DEPARTMENT OF DEFENSE POLICIES OR POSITIONS. THERE IS NO SUCH THING AS A PERSONAL OR UNOFFICIAL HOME PAGE ON A ".MIL" SERVER BECAUSE THESE SERVERS AND THE INFORMATION THEY CONTAIN ARE PROPERLY USED ONLY FOR OFFICIAL BUSINESS, AND IN AN OFFICIAL CAPACITY. COMMANDING OFFICERS SHOULD REVIEW ALL WEB HOME PAGES OR OTHER INTERNET INFORMATION SERVERS BEING OPERATED BY PERSONNEL AT THEIR COMMANDS , TO ENSURE COMPLIANCE WITH THE GUIDELINES NOTED IN THIS MESSAGE.

6. ADDITIONAL MORE DETAILED TECHNICAL AND INFOSEC GUIDELINES PERTAINING TO DON USE OF THE INTERNET WILL BE PUBLISHED IN FUTURE REVISIONS TO REFS D AND E.

7. THIS MESSAGE HAS BEEN COORDINATED WITH CMC, CHINFO, NAVY JAG, AND COMNAVSECGRU. THE N6 POINT OF CONTACT IS CDR D. GALIK, N643G. PHONE 703 697-7755, OR EMAIL: CNON643G@SMTP-GW.SPAWAR.NAVY.MIL. THE MARINE CORPS POINT OF CONTACT IS MARINE CORPS COMBAT DEVELOPMENT COMMAND, ARCHITECTURE AND STANDARDS DIVISION; PHONE 703 784-4720.

8. RELEASED BY VADM DAVIS, USN.//

BT

DEPARTMENT OF THE NAVY

ENLISTED PERSONNEL MANAGEMENT CENTER

NEW ORLEANS, LOUISIANA 70159-7900

iN REPLY REFER TO
October 10, 1996

MEMORADUM FOR DEPARTMENT DIRECTORS - 56-06

Subj: USE OF FEDERAL GOVERNMENT RESOURCES

Ref: (a) DOD 5500.7-R (Second Amendment 3/25/96)

Encl: (1) Joint Ethics Regulation, Chapter 2, Section 1, 2-301

1. Per reference (a) significant changes have been made to government policy for use of resources. Updated DOD changes are in enclosure (1). The following is EPMAC's Command Policy:

a. FEDERAL GOVERNMENT COMMUNICATION SYSTEMS AND EQUIPMENT (telephones, facsimile machines, electronic mail, internet system)

(1) Authorized purposes allow for brief personal communication such as checking with spouse or minor children, scheduling doctor and auto or home repair appointments, brief internet searches, e-mailing directions to visiting relatives, under the following criteria:

(a) Do not adversely affect the performance of official duties.

(b) Are of reasonable duration and frequency and whenever possible are made during the employee's personal time such as after duty hours or lunch periods.

(c) Serve a legitimate public interest such as keeping employees at their desks rather than requiring the use of commercial systems, educating employees on the use of communication systems, improving morale of employees, job-searching in response to downsizing.

(d) Do not overburden the communication system, create no significant additional cost to the government, and in the case of long distance communication charges are: charged to employee's home number or personal telephone credit card, made t

OTTUZYUW RUEKJCS0329 2101731-UUUU--RUCCNOM RUCCNOP.
ZNR UUUUU
O 281928Z JUL 97 PSN 233875J28
FM SECDEF WASHINGTON DC//OASD:PA/DPL//
TO AIG 8775
INFO RUEKJCS/SECDEF WASHINGTON DC//OASD(PA)//
BT
UNCLAS
SUBJECT: DOD WEB SITE POLICY RELEASED

1. THE OFFICES OF THE ASSISTANT SECRETARIES OF DEFENSE FOR PUBLIC AFFAIRS AND FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE RECENTLY COMPLETED AN UPDATE TO THE POLICY FOR ESTABLISHING AND MAINTAINING A PUBLICLY ACCESSIBLE DOD WEB INFORMATION SERVICE, COMMONLY KNOWN AS A WEB SITE.

2. THE POLICY, WHICH IS EFFECTIVELY IMMEDIATELY, APPLIES TO THE OFFICE OF THE SECRETARY OF DEFENSE, THE MILITARY DEPARTMENTS, THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF, THE COMBATANT COMMANDS, THE DEFENSE AGENCIES AND THE DOD FIELD ACTIVITIES.

3. THE DOCUMENT IS AVAILABLE ONLINE AT: HTTP://WWW.DTIC.MIL/DEFENSELINK/ABOUT.HTML (ALL LOWERCASE), ALONG WITH LINKS TO THE VARIOUS SERVICE POLICIES.

4. THE DOD POLICY IS THE RESULT OF EXTENSIVE COORDINATION WITH ALL

PAGE 02 RUEKJCS0329 UNCLAS

THE MILITARY SERVICES AND OTHER REPRESENTATIVES TO THE DOD TECHNOLOGY WORKING GROUP, CHAIRED BY OASD(PA). FOR SERVICE QUESTIONS, COMMENTS OR SUGGESTIONS ON THE POLICY, CONTACT YOUR RESPECTIVE REPRESENTATIVE TO THE TECHNOLOGY WORKING GROUP. DOD: JKNOTTS@PAGATE.PA.OSD.MIL; ARMY: WEBMASTER@HQDA.ARMY.MIL; AIR FORCE: HUBBARDB@AF.PENTAGON.MIL; NAVY: WEBMASTER@CHINFO.NAVY.MIL; MARINE CORPS: DONALDSONW1@MQG-SMTP3.USMC.MIL. ALL OTHERS CAN CONTACT THE PERSON WITHIN YOUR AGENCY OR ACTIVITY THAT DEALS WITH INTERNET POLICY.

5. OASD(PA) POINT OF CONTACT IS CAPTAIN JIM KNOTTS, USAF, (703) 697-3532, DSN 227-3532, EMAIL JKNOTTS@PAGATE.PA.OSD.MIL.

BT
#0329
NNNN

DEPARTMENT OF THE NAVY
NAVAL INFORMATION SYSTEMS
MANAGEMENT CENTER

NAVSO P-5239-29
JULY 1994

CONTROLS OVER COPYRIGHTED COMPUTER SOFTWARE

GUIDEBOOK

MODULE 29

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

EPMAC

650-97

DEPARTMENT OF THE NAVY

NAVAL INFORMATION SYSTEMS MANAGEMENT CENTER
1225 JEFFERSON DAVIS HIGHWAY
ARLINGTON VIRGiNIA 22202-4311

Ser: 03/97-0040

MAR 27 1997

MEMORANDUM FOR DISTRIBUTION

Subj: POLICY ON DEPARTMENT OF DEFENSE (DOD) ELECTRONIC NOTICE AND CONSENT BANNER

Encl: (1) ASD(C3I) memo of 16 Jan 97

Enclosure (1) is forwarded for appropriate action. DOD policy directs that all DOD automated information systems (AISs) must display an electronic log-on notice and consent banner that advises:

- the system is a DOD system;
- the system is subject to monitoring;
- monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures; and
- use of the system constitutes consent to monitoring.

All users should be made aware of the policy regarding AIS monitoring, and all AISs now in use are required to automatically display a notice and consent banner by 16 April 1997.

Please ensure that this policy is widely distributed throughout your organization and those organizations that report to you.

Stephen I. Johnson

STEPHEN I. JOHNSON
Rear Admiral, U.S. Navy

Distribution:
CNO
CMC
CINCLANTFLT
CINCPACFLT
CINCUSNAVEUR
GC
ASN(MR&A)
ASN(FM&C)
ASN(I&E)
ASN(RD&A)
COMNAVAIRSYSCOM
COMNAVFACENGCOM
COMNAVSEASYSCOM
COMSPAWARSYSCOM
COMNAVSUPSYSCOM
COMARCORPSYSCOM
(cont. next pg.)

COPY FOR YOUR INFORMATION

GM

RTAUZYUW RUENAAA0160 2841912-UUUU--RUCRNAA.
ZNR UUUUU
R 1117542 OCT 95 ZYB MIN
FM CNO WASHINGTON DC//N6//
TO ALCOM

UNCLAS //N03264//
ALCOM 045/95
MSGID/GENADMIN/CNO WASH DC N643//
SUBJ/DEPARTMENT OF THE NAVY POLICY FOR COMPUTER INCIDENT RESPONSE AND
/VULNERABILITY REPORTING//
REF/A/DOC/NTISSP/930830//
REF/B/DOC/NTISSD/930830//
REF/C/DOC/CNO/850401//
NARR\REF A IS NATIONAL SECURITY AND TELECOMMUNICATIONS AND
INFORMATION SYSTEMS SECURITY POLICY (NSTISSP) NUMBER 5, NATIONAL
POLICY FOR INCIDENT RESPONSE AND VULNERABILITY REPORTING FOR NATIONAL
SECURITY SYSTEMS. REF B IS NATIONAL SECURITY TELECOMMUNICATIONS AND
INFORMATION SYSTEMS SECURITY DIRECTIVE (NSTISSD) NUMBER 503, INCIDENT
RESPONSE AND VULNERABILITY REPORTING FOR NATIONAL SECURITY SYSTEMS.
REF C IS OPNAVINST 5239.1, DON ADP SECURITY POLICY.//
POC/CDR D. GALIK/CNO N643G/-/-/TEL:(703)697-7755//
PAGE 02 RUENAAA0160 UNCLAS
RMKS/1. RECENT EVENTS INVOLVING THE USE OF INTERNATIONAL
TELECOMMUNICATIONS AND NETWORK COMPUTER SYSTEMS-TO ATTEMPT TO EXPLOIT
AND DISRUPT DOD INFORMATION SYSTEMS, CLEARLY UNDERSCORE THE NEED FOR
AN ORGANIZED AND FULLY SUPPORTED CAPABILITY TO DEAL WITH SUCH
INCIDENTS. REF A DIRECTED THAT U. S. GOVERNMENT DEPARTMENTS AND
AGENCIES COLLABORATE AND COORDINATE EFFORTS TO:
A. CONTAIN AND MINIMIZE THE IMPACT OF SECURITY INCIDENTS ON
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS, AND
B. ELIMINATE OR MINIMIZE VULNERABILITIES AMONG NATIONAL
SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS.
REF B ALSO DIRECTED THAT A SECURITY INCIDENT RESPONSE CAPABILITY BE
ESTABLISHED AT THE SERVICE/AGENCY LEVEL, TO PROVIDE EXPERT ASSISTANCE
IN ISOLATING, CONTAINING, AND ELIMINATING INCIDENTS THAT THREATEN THE
INTEGRITY, AVAILABILITY, OR CONFIDENTIALITY OF OUR SYSTEMS.
2 . THIS MESSAGE PROVIDES DEPARTMENT OF THE NAVY (DON) POLICY THAT
REQUIRES THE REPORTING OF ALL SECURITY INCIDENTS DEFINED HEREIN
INVOLVING DON AUTOMATED INFORMATION SYSTEMS (AIS) AND NETWORKS, TO
THE NAVAL COMPUTER INCIDENT RESPONSE TEAM (NAVCIRT). AIS SECURITY
INCIDENT REPORTING PROCEDURES FOR SERVICE CRYPTOLOGIC ELEMENT (SCE)
SYSTEMS IS PROVIDED IN SUPPLEMENT 1 TO NSA/CSS MANUAL 130-1, WHICH
PAGE 03 RUENAAA0160 UNCLAS
IDENTIFIES COMNAVSECGRU AS THE FOCAL POINT. COMNAVSECGRU WILL

```
- - - - - - - - - - - - ASSIST.DOC follows - - - - - - - - - - - -
MAIL From: <assist -owner@assist.mil>
RCPT  To:<STASCHKB@GW.EPMAC.NOLA.NAVY.MIL>
Received: by atlanta.assist.mil (8.8.5/LOCAL-4.0)
        id XAA04585; Mon, 11 Aug 1997 23:52:53 GMT
From: assist-owner@assist.mil
Date: Mon, 11 Aug 1997 23:40:20 GMT
Message-Id: <199708112340.XAA03566@antietam.assist.mil>
Errors-To: assist-owner@assist.mil
X-Sender: 227
Subject: ASSIST Advisory# 97-10: DOD site licensed Anti-Virus tools
To: assist-bulletins@assist.mil
Sender: assist-owner@assist.mil
Precedence: bulk
Reply-To: assist@assist.mil
```

```
-----BEGIN PGP SIGNED MESSAGE -----

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
         Automated Systems Security Incident Support Team

                                                      |     /
             ____   ____   _____   ____   _____       |    /  Integritas
      /\    /    \ /    \    |    /    \    |         |   <      et
     /  \   \____  \____     |    \____     |         |    \  Celeritas
    /____\       \      \    |         \    |         |_____\
          \ \____/ \____/  __|__  \____/    |
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
```

ADVISORY : 97-10

Release date: 11 Aug, 1997

DESCRIPTION: DOD site licensed Anti-Virus (AV) tools.

SUMMARY: The McAfee and Symantec Norton computer AV software has been site licensed for use by DOD and will be available for use as of 1 September 97. The software will be available for use by the DOD antivirus support community on 15 August 97. The DOD license was procured by the Defense Information Systems Agency (DISA) contract DCA100-98-F-0004 to Stream International (Symantec's Norton AntiVirus) and DCA100-98-F-0005 to McAfee is valid through 30 Sept 98.

BACKGROUND: The DOD site license for the IBMAV and Norman software expires on 30 September 97. DOD personnel may continue to use the IBMAV software after the expiration date, however virus signature updates will no longer be issued.

IMPACT: Failure to maintain and use an up to date AV tool places systems at risk of malicious code infection.

RECOMMENDED SOLUTIONS: Obtain, install, and begin using the DOD site
licensed McAfee and Norton AV tool as soon as possible.
Ensure the AV tool is kept up to date by obtaining and installing the most current version of the software as soon as it is available from the DOD distribution centers.

Army: Army Computer Emergency Response Team (ACERT)
Hotline: 1-888-203-6332 (DSN: 235-1113)
Anonymous FTP: ftp.acert.belvoir.army.mil
Web Server: http://www.acert.belvoir.army.mil

Navy: NISE East, Charleston, SC Information Systems Security (INFOSEC)
Technical Help Desk: 800-304-4636
Anonymous FTP: INFOSEC.NOSC.MIL (198.253.23.241)
BBS: 800-494-9947 (DSN 764-2474)

Air Force: Air Force Information Warfare Center (AFIWC)

Anonymous FTP: afcert.csap.af.mil (192.203.2.249),

AFCA C4 Systems Security BBS: 618-256-4545 (DSN 576-4545)

Other: Automated Systems Security Incident Support Team (ASSIST)
Hotline: (800) 357-4231 (DSN: 327-4700)
Anonymous FTP: ftp.assist.mil (199.211.123.12)
Web Server: http://www.assist.mil (199.211.123.12)

Personnel from each DOD element should download the" software from their respective MILDEP distribution centers. Personnel affiliated with non–MILDEP elements should use the ASSIST BBS or FTP servers.

****

The following is a copy of the license terms, conditions and coverage: DOD–Wide Anti-Virus Software Enterprise License Agreement Between Defense Information Systems Agency and McAfee Software, Inc.

1. Agreement: This software license agreement is entered into on this date, 16 July 1997, between the Defense Information Systems Agency, hereinafter referred to as DISA, and the anti-virus software manufacturer/developer, McAfee Software, Inc., hereinafter referred to as the Contractor to furnish the

following anti–virus software product or products: Virus Scan, NetShield, WebShield, BootShield, GroupShield, and GroupScan and WebScan.

2. Order of Precedence: The terms of this license agreement are a supplement to the Contractor's commercial license for the aforementioned product(s) and should any conflict arise between the two agreements, the terms of this agreement shall take precedence.

3. Coverage/Applicability: This license covers the entire Department of Defense (DOD) on a Perpetual, Enterprise basis during the Period of Performance of this license, including Technical Support, Distribution, and Home Use as defined below.

4. Definitions:

Period of Performance: This license covers the period from date of award through 30 September 1998, plus four additional one year options, if exercised by DISA.

Option prices: $410,000 per option period for a total license value of $2,050,000 if all 4 options are exercised.

DOD: For the purposes of this license this includes all employees of, and PC's owned by the: Army, Air Force, Navy, Marines, Coast Guard (in time of war only), defense agencies, military academies (on–site/campus only). It may be used by DOD contractors working on DOD owned PC's but not by DOD Contractors working on their company-owned PC's at their workplace.

Perpetual: This product is for DOD's use only, in perpetuity, however, anti–virus software technical support and signature file updates stop at the end of the designated period of the license. This also means that there is no requirement to de-install, destroy and/or return to the Contractor installed software at the end of the license period.

Enterprise This software is always owned by the software developer (Contractor) and is only used by the DOD, with no requirement to: account for or report individual DOD users or software copies, increase or decrease the price based on changes in the number of DOD users or PC'S, and covers all product updates or upgrades based on new versions of operating systems or new platforms that occur for products originally provided under this license, during the period of this license.

Home use: DOD Employees only may use the anti-virus product on their own personal computers at their homes. This is to reduce incidents of virus infiltration from home computers owned by DOD Employees where a significant virus point-of-entry exists. It may not be used by DOD Contractors at their own home.

Technical support (and/or maintenance support): This includes any or all technical support normally associated with or provided with the commercial version of the product(s), to the Contractor's commercial market. This will include a 24 hour-7 day-a-week accessible technical support hot line. The Contractor is only required to furnish technical support under this license to the DISA ASSIST staff. In addition, the contractor will agree to accept technical support calls from DOD Activity Information Security and/or network systems administrators after coordination with or after being referred to by the ASSIST Staff.

Distribution: Software updates, signature updates, system administrator documentation, virus logging, reporting, as well as end-user software documentation covered by this license shall be primarily via contractors commercial automatically or manually downloadable FTP, INTERNET/web, or bulletin board site, by and distributed by DISA ASSIST staff or other mutually agreed–to method. In addition, a hard copy set of software updates and/or virus solutions shall be furnished as soon as available in the form of CD ROM(s), and/or 3 1/2 inch Diskette(s) and shall be shipped via express mail (or equivalent) to the DISA ASSIST staff.

5 . Changes: Signatures below constitute the entire agreement of this addendum between DISA and the Contractor. Any or all changes to this agreement must be made in writing by mutual agreement of the undersigned or their authorized representatives.

ADDENDUM TO SYMANTEC'S RETAIL LICENSE AND WARRANTY

This Addendum to License and Warranty (the "Addendum") dated 16 July 1997 shall serve to amend the standard retail package product License and Warranty (the "Agreement") which accompanies Symantec's Antivirus packaged product which will govern the Symantec Software Product purchased by the Defense Information Systems Agency, ("DISA"), pursuant to the GSA Schedule buy of a DOD–wide antivirus software license. DISA is the purchasing agency for the Department of Defense ("DOD"). The terms of the

Addendum shall control in the event of arty conflict between the Agreement and the Addendum.

The Agreement will be amended as follows.

1. Notwithstanding anything to the contrary specified in the Agreement, Symantec grants to DOD a nonexclusive, nontransferable license to make and use an unlimited number of copies of the English language versions of the Software in object code form only, solely for DOD's own internal data processing uses within the United States (and includes the international addendum for DOD use overseas). The licenses covered by the Agreement and this Addendum are perpetual in nature. Upgrade Insurance and PremiumCare Platinum Support (24X7 option, 6 designated persons) will be provided under the terms and conditions of Symantec's Upgrade Insurance and PremiumCare Platinum agreements for the term of the Agreement.

2. Notwithstanding anything to the contrary specified in the Agreement, employees of DOD who have been provided a copy of the Software for office use may also use a duplicate copy of such Software under the terms and conditions of the Agreement on their home computers so long as they remain employed by DOD.

3. DOD computers will include all computers owned by the Army, Air Force, Navy, Marines, Coast Guard (in time of war only), Defense agencies, Military Academies (on-site/campus only). DOD computers will include contractors working on DOD owned computers but not DOD contractors working on their company-owned computers at their workplace or at their home.

4. The terms of the Agreement and this Addendum shall begin from the date of execution by both parties through September 30, 1998. DOD will have the option to renew the Agreement for up to four additional one year periods. The pricing for the Software will be determined by Stream and DOD for the initial term as well as the option terms.

5. This Addendum and the Agreement constitute the entire understanding of the parties regarding the subject matter hereof and may be modified or waived only by a writing duly executed on behalf of both parties. No purchase order, invoice or similar memorandum will amend the Agreement or this Addendum even if accepted in writing by the receiving party.

Access to the McAfee and Norton AV tools on the ASSIST BBS, FTP and Web servers is restricted to DOD verified personnel only. Any DOD component that further distributes the DOD licensed AV tools electronically must also verify that recipients are DOD affiliated personnel. Failure to comply with contract guidelines will put the distributor in violation of the contract. See “ASSIST Information Resources” section in the trailer of this message and ASSIST 97–1 for additional information about downloading files from ASSIST, and DOD-only restricted access to AV tools. Please contact ASSIST if you encounter any problems downloading files from the ASSIST BBS, FTP, WebServer systems.

ASSIST will act as the sole DOD liaison with McAfee and Norton AV software, for all matters related to DOD use of the McAfee and Norton AV tools. All questions, comments, problems, and suggestions related to DOD use of the McAfee and Norton AV tools must be forwarded through the MILDEP representatives listed below to ASSIST, and non-MILDEP DOD personnel must contact ASSIST directly.

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

ASSIST is an element of the Defense Information Systems Agency (DISA), Global Operations and Security Center (GOSC), which provides
service to the entire DoD community. Constituents of the DoD with questions about ASSIST or computer security issues, can contact ASSIST
using one of the methods listed below. Non-DoD organizations/institutions, contact the Forum of Incident Response and
Security Teams (FIRST) representative. To-obtain a list of FIRST member organizations and their constituencies send an email to docserver@first.org with an empty “subject” line and a message body containing the line “send first-contacts”.

____
ASSIST CONTACT INFORMATION:

E-mail: assist@assist.mil
Phone: (800)-357-4231 (DSN 327-4700) 24 hour hotline
Fax: (703) 607-4735 (DSN 327-4735) Unclassified

ASSIST Bulletins, tools and other security related information are available from:
    http://www.assist.mil/
    ftp://ftp.assist.mil/

To be added to our mailing list for ASSIST bulletins, send your e-mail
address to:
    assist–request@assist.mil
In the subject line, type:
    SUBSCRIBE your–email–address

____
OTHER DOD CERT CONTACT INFORMATION:

Air Force CERT Phone: (800) 854-0187
Air Force CERT Email: afcert@afcert.csap.af.mil

Navy CIRT Phone: (800) 628-8893
Navy CIRT Email: navcirt@fiwc.navy.mil

Army CERT Phone: (888) 203-6332
Army CERT Email: acert@vulcan.belvoir.army.mil

Stratcom CERT Phone: (402) 294-1985
Stratcom Email: stratcert@stratcom.af.mil

ASSIST BULLETINS:

Back issues of ASSIST bulletins, and other security related information, are available from the ASSIST BBS at 703-607-4710, 327-4710, and through anonymous FTP from ftp.assist.mil (IP address 199.211.123.12). Note: ftp.assist.mil will only accept anonymous FTP connections from Milnet addresses that are registered with the NIC or DNS. If your system is not registered, you must provide your MILNET IP address to ASSIST before access can be provided.

ASSIST uses Pretty Good Privacy (PGP) as the digital signature mechanism for bulletins. PGP incorporates the RSAREF(tm) Cryptographic Toolkit under license from RSA Data Security, Inc. A copy of that license is available via anonymous FTP from net-dist.mit.edu (IP 18.72.0.3) in the file /pub/PGP/rsalicen.txt. In accordance with the terms of that license, PGP may be used for non-commercial purposes only. Instructions for downloading the PGP software can also be obtained from net-dist.mit.edu in the pub/PGP/README file. PGP and RSAREF may be subject to the export control laws of the United States of America as implemented by the United States Department of State Office of Defense Trade Controls. The PGP signature information will be attached to the end of ASSIST bulletins.

Reference herein to any specific commercial product, process, or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by ASSIST. The views and opinions of authors expressed herein shall not be used for advertising or product endorsement purposes.

```
-----BEGIN PGP SIGNATURE -----
Version: 2.6
```

DEPARTMENT OF THE NAVY

NAVSO P-5239-19
AUGUST 1996

COMPUTER INCIDENT RESPONSE GUIDEBOOK

MODULE 19

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

NAVAL RESERVE
LOGISTIC SUPPORT HANDBOOK

COMMANDER NAVAL RESERVE FORCE
NEW ORLEANS, LOUISIANA

DEPARTMENT OF THE NAVY
Office of the Secretary
Washington, DC 20350-1000

SECNAVINST 5211.5D
OP-09B30
17 July 1992

SECNAV INSTRUCTION 5211.5D

From: Secretary of the Navy
To: All Ships and Stations

Subj: DEPARTMENT OF THE NAVY PRIVACY ACT (PA) PROGRAM

Ref:
(a) 5 U.S. C. 552a, as amended by the computer Matching Act of 1988
(b) DOD Directive 5400.11 of 9 Jun 82, DOD Privacy Program (NOTAL)
(c) DOD Regulation 5400.11-R of 31 Aug 83, "DOD Privacy Act Program" (NOTAL)
(d) 5 U.S. C. 552 (1988) as amended by the Freedom of Information Reform Act of 1986
(e) SECNAVINST 5720.42E, Department of the Navy Freedom of Information Act Program
(f) OPM Regulations and the Federal Personnel Manual
(g) 42 U.S. C. 653, Parent Locator Service for Enforcement of Child Support

Encl:
(1) Table of Contents
(2) Contents of Record System Notice and Sample Report on New System of Records Format
(3) Sample Report on Altered System of Records Notice and Format
(4) Contents of an Amended Systems of Records Notice and Format
(5) Contents of a Deleted Systems of Records Notice and Format
(6) Special Considerations for Using and Safeguarding Records in Computerized Systems of Records
(7) Special Considerations for Safeguarding Records during Word Processing
(8) General Purpose Privacy Act Statement (OPNAV 521 1/12 (3/92))
(9) DOD Blanket Routine Uses
(10) Disclosure Accounting Form (OPNAV 5211/9 (3-92))
(11) List of Exempt Systems
(12) Sample Exemption Rule
(13) Provisions of the PA from Which a General or Specific Exemption May Be Claimed
(14) Litigation Status Report
(15) Sample Training Package and Slides
(16) Instructions for Preparing OPNAV Form 5211/10, Annual Report - Privacy Act
(17) Sample Checklist for Conducting PA Staff Assistance Visits
(18) Computer Matching Guidelines
(19) Text of Privacy Act of 1974 (As Amended) - 5 U.S.C. 552a

1. Purpose

a. To provide Department of the Navy (DON) policies and procedures for:

(1) -Governing the collection, safeguarding, maintenance, use, access, amendment, and dissemination of personal information kept by DOS in systems of records;

(2) Notifying individuals if any systems of records contain a record pertaining to them;

(3) Verifying the identity of individuals who request their records before the records are made available to them;

(4) Notifying the public of the existence and character of each system of records.

(5) Exempting systems of records from certain requirements of the PA; and

(6) Governing the PA rules of con–duct for DON personnel, who will be subject to criminal penalties for noncompliance with reference (a).

PUBLIC LAW 100-235—JAN. 8, 1988

COMPUTER SECURITY ACT OF 1987

19-139 O - 88 - (235)

Public Law 100-235
100th Congress

An Act

Jan. 8, 1988
[H.R. 145]

To provide for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Computer Security Act of 1987.
Classified information.
40 USC 759 note.
40 USC 759 note.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Act of 1987".

SEC. 2. PURPOSE.

(a) In General.—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) Specific Purposes.—The purposes of this Act are—

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended—

15 USC 272.

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof: "; and", and by inserting after such paragraph the following:

"(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.";

15 USC 278h.

(2) by redesignating section 20 as section 22, and by inserting after section 19 the following new sections:

15 USC 278g-3.

"Sec. 20. (a) The National Bureau of Standards shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

"(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987; Regulations.

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) For the purposes of—

"(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

"(2) performing research and conducting studies under subsection (b)(5),

the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

"(d) As used in this section—

"(1) the term 'computer system'—

"(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

"(B) includes—

"(i) computers;

"(ii) ancillary equipment;

"(iii) software, firmware, and similar procedures;

"(iv) services, including support services; and

"(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

"(2) the term 'Federal computer system'—

"(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

"(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

"(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

"(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

15 USC 278g-4.

"SEC. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be—

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

Reports.

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

"(c) The term of office of each member of the Board shall be four years, except that—

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board

Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

"(g) As used in this section, the terms 'computer system' and 'Federal computer system' have the meanings given in section 20(d) of this Act."; and

(3) by adding at the end thereof the following new section:

National Bureau of Standards Act.
15 USC 271 note.

"SEC. 23. This Act may be cited as the National Bureau of Standards Act.".

SEC. 4. AMENDMENT TO BROOKS ACT.

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows:

"(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

President of U.S.

Federal Register, publication.

"(2) The head of a Federal agency may employ standards for the cost-effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by Government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental

Federal Register, publication.

Affairs of the Senate and shall be published promptly in the Federal Register.

"(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection. Regulations.

"(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act.".

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

40 USC 759 note.

(a) In General.—Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be—

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) Training Objectives.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) Regulations.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.

40 USC 759 note.

(a) Identification of Systems That Contain Sensitive Information.—Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) Security Plan.—Within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

40 USC 759 note.

SEC. 7. DEFINITIONS.

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information", and "Federal agency" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

40 USC 759 note.

SEC. 8. RULES OF CONSTRUCTION OF ACT.

Nothing in this Act, or in any amendment made by this Act, shall be construed—

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

Public information.

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

Approved January 8, 1988.

LEGISLATIVE HISTORY—H.R. 145:

HOUSE REPORTS: No. 100-153, Pt. 1 (Comm. on Science, Space, and Technology) and Pt. 2 (Comm. on Government Operations).

CONGRESSIONAL RECORD, Vol. 133 (1987):
June 22, considered and passed House.
Dec. 21, considered and passed Senate.